FINITE FIELDS AND THEIR APPLICATIONS **3,** 159–174 (1997)
ARTICLE NO. FF970181

Linear Complexity of Generalized Cyclotomic Binary Sequences of Order 2

Cunsheng Ding

Turku Centre for Computer Science, Lemminkaisenkatu 14 A, DataCity,

Communicated by Harald Niederreiter

Received July 22, 1996; revised December 24, 1996

There are several kinds of cyclotomic sequences. They have a number of good randomness properties. In this paper we calculate the linear complexity (linear span) of generalized cyclotomic binary sequences of order 2. Our results show that their linear complexity is quite good. © 1997 Academic Press

I. INTRODUCTION

There are different kinds of cyclotomic sequences and they have quite good randomness properties [4]. Examples of such sequences are the generalized cyclotomic sequences of order 2 [4].

An integer a is called a primitive root of (or modulo) n if the multiplicative order of a modulo n, denoted by $\mathrm{ord}_n(a)$, is equal to $\phi(n)$, where $\phi(x)$ denotes the Euler function and $\gcd(a, n) = 1$.

Let p and q be two odd primes with $d = \gcd(p - 1, q - 1)$. Define $e = (p - 1)(q - 1)/d$. It is well known that a prime p has $\phi(p - 1)$ primitive roots. The Chinese Remainder Theorem guarantees that there are common primitive roots of both p and q. Let g be a fixed common primitive root of both p and q, and let x be an integer satisfying.

$$x \equiv g \pmod{p}, \qquad x \equiv 1 \pmod{q}.$$

Whiteman proved that [19]

$$Z_{pq}^{*} = \{g^s x^i : s = 0, 1, \ldots, e - 1; i = 0, 1, \ldots, d - 1\},$$

1071-5797/97 $25.00

where Z_{pq}^* denotes the set of all invertible elements of the residue class ring Z_{pq}. The generalized cyclotomic classes D_i of order d with respect to p and q are defined by

$$D_i = \{g^s x^i : s = 0, 1, \ldots, e-1\} \qquad i = 0, 1, \ldots, d-1.$$

It is not hard to prove that [19]

$$Z_{pq}^* = \bigcup_{i=0}^{d=1} D_i, \qquad D_i \cap D_j = \Phi \qquad \text{for } i \neq j,$$

where Φ denotes the empty set. This kind of generalized cyclotomy was introduced by Whiteman [19]. The motivation behind the investigation of the generalized cyclotomy with respect to two primes is the search for residue difference sets. The famous twin-prime difference sets are among such a class of difference sets. For details about classical cyclotomies we refer to [6, 1, 17].

Let S be a subset of Z_{pq} and let a an element of Z_{pq}. Define

$$S \pm a = \{s \pm a : s \in S\}, \qquad a \cdot S = \{a \cdot s : s \in S\},$$

where "$\pm$" and "$\cdot$" denote the integer addition modulo pq, integer subtraction modulo pq, and integer multiplication modulo pq, respectively. We also use $a \bmod n$ to denote the least nonnegative integer that is congruent to a modulo n.

In the sequel we shall only consider the case that $d = \gcd(p-1, q-1) = 2$. In this case D_0 and D_1 are called cylotomic classes of order 2. For simplicity we define $N = pq$. Define

$$P = \{p, 2p, \ldots, (q-1)p\}, \qquad Q = \{q, 2q, \ldots, (p-1)q\}.$$
$$R = \{0\}, \qquad C_0 = R \cup Q \cup D_0, \qquad C_1 = P \cup D_1.$$

Then

$$C_0 \cup C_1 = Z_{pq}, \qquad C_0 \cap C_I = \Phi.$$

The generalized cylotomic binary sequences s^∞ of order 2 with respect to the primes p and q is defined as

$$s_i = \begin{cases} 0, & \text{if } (i \bmod N) \in C_0, \\ 1, & \text{if } (i \bmod N) \in C_1, \end{cases} \text{ for all } i \geq 0.$$

It is easy to see that this sequence can be expressed as $s_i = F(i \bmod N)$ with

$$F(i) = \begin{cases} 0, & i \in R \cup Q, \\ 1, & i \in P, \\ \left(1 - \left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\right)/2, & \text{otherwise.} \end{cases} \text{ for all } 0 \le i \le N-1, \quad (1)$$

where (a/p) denotes the Legendre symbol.

The autocorrelation properties of these sequences are determined by the generalized cyclotomic numbers of order 2 [4]. Lower bounds on the linear complexity of these sequences are presented in [4]. But those lower bounds on the linear complexity of these sequences depend on special properties of the primes. In this paper we calculate the exact value of the linear complexity of these sequences in general without any special requirement about the primes.

2. LINEAR COMPLEXITY AND MINIMAL POLYNOMIAL

Let $s^\infty = s_0 s_1 \cdot \cdot \cdot s_{n-1} \cdot \cdot \cdot$ be a periodic infinite sequence over a field F. The linear complexity or linear span of s^∞ is defined to be the least positive integer l such that there are constants $c_0 = 1, c_1, \cdot \cdot \cdot, c_l \in F$ satisfying

$$-s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdot \cdot \cdot + c_l s_{i-l} \qquad \text{for all } i \ge l.$$

The polynomial $c(x) = c_0 + c_1 x + \cdot \cdot \cdot + c_l x^l$ is called a minimal polynomial of s^∞ or, in engineering terms, the feedback polynominal of a shortest linear feedback shift register that produces the sequence. Such a polynomial and l always exist for a periodic infinite sequence. The linear complexity of periodic sequences can be expressed simply as follows.

Let s^∞ be a sequence of period n over a field F, and

$$S^n(x) = s_0 + s_1 x + \cdot \cdot \cdot + s_{n-1} x^{n-1}.$$

It is well known that [7]

1. the minimal polynomial of s^∞ is given by

$$(x^n - 1)/\gcd(x^n - 1, S^n(x)); \quad (2)$$

2. the linear complexity of s^∞ is given by

$$n - \deg(\gcd(x^n - 1, S^n(x))). \quad (3)$$

Linear complexity is an important measure of the strength of keystream sequences for additive synchronous stream ciphering and also a measure of the randomness of sequences [3, 8–11].

To compute the linear complexity of the sequence, we need a number of lemmas.

LEMMA 1. *Let the symbols be the same as before. Then*

1. $\mathrm{ord}_N(g) = e$, *where* $\mathrm{ord}_N(g)$ *denotes the order of* g *modulo* N.
2. D_0 *is a group with respect to the integer multiplication modulo* pq.
3. *If* $a \in D_0$ *then* $aD_1 = D_1$ *and* $aD_0 = D_0$; *if* $a \in D_1$ *then* $aD_1 = D_0$ *and* $aD_0 = D_1$.

Proof. Since g is a common primitive root of both p and q, by the Chinese Remainder Theorem

$$\begin{aligned}\mathrm{ord}_N(g) &= \mathrm{lcm}\{\mathrm{ord}_p(g), \mathrm{ord}_q(g)\}\\ &= \mathrm{lcm}\{p-1, q-1\}\\ &= (p-1)(q-1)/d = e.\end{aligned}$$

This proves part one.

The second part follows easily from part one and the definition of D_0.

Since $x \in Z_N^*$, there must exist an integer u with $0 \le u \le e-1$ such that $x^2 = g^u$. If $a \in D_1$, there must exist a v such that $a = g^v x$. It follows that

$$\begin{aligned}aD_1 &= \{g^{s+v}x^2 : s = 0, 1, \ldots, e-1\}\\ &= \{g^{s+v+2} : s = 0, 1, \ldots, e-1\}\\ &= D_0.\end{aligned}$$

The remaining parts can be similarly proved. ■

Let m be the order of 2 modulo N. Then the field $GF(2^m)$ has a primitive Nth root of unity. Define

$$S(x) = \sum_{i \in C_1} x^i = \left(\sum_{i \in P} + \sum_{i \in D_1}\right) x^i \in GF(2)[x].$$

By (2) we now compute $\gcd(x^N - 1, S(x))$. To this end, we need a few auxiliary results.

Let θ denote such a primitive Nth root of unity over $GF(2^m)$, we have

$$0 = \theta^N - 1 = (\theta^p)^q - 1 = (\theta^p - 1)(1 + \theta^p + \theta^{2p} + \cdots + \theta^{(q-1)p}).$$

It follows that

$$\theta^p + \theta^{2p} + \cdots + \theta^{(q-1)p} = 1. \tag{4}$$

By symmetry we get

$$\theta^q + \theta^{2q} + \cdots + \theta^{(p-1)q} = 1. \tag{5}$$

LEMMA 2. *Let the symbols be the same as before. Then*

$$\sum_{i \in D_1} \theta^{ai} = \begin{cases} \left(\dfrac{p-1}{2} \bmod 2\right), & \text{if } a \in P, \\ \left(\dfrac{q-1}{2} \bmod 2\right), & \text{if } a \in Q, \end{cases}$$

Proof. Suppose that $a \in Q$. Since g is a common primitive root of both p and q and the order of g modulo N is e, by the definition of x we have

$$\begin{aligned} D_i \bmod p &= \{g^s x^i \bmod p : s = 0, 1, \ldots, e-1\} \\ &= \{g^{s+i} \bmod p : s = 0, 1, \ldots, e-1\} \\ &= \{1, 2, \ldots, p-1\}. \end{aligned}$$

When s ranges over $\{0, 1, \ldots, e-1\}$, $g^s x^i \bmod p$ takes on each element of $\{1, 2, \ldots, p-1\}$ $(q-1)/2$ times. It follows from (4) that

$$\begin{aligned} \sum_{j \in D_1} \theta^{aj} &= \left(\frac{q-1}{2} \bmod 2\right) \sum_{j \in Q} \theta^j \\ &= \left(\frac{q-1}{2} \bmod 2\right). \end{aligned}$$

The rest of the conclusion of this lemma can be similarly proved. ∎

LEMMA 3. *Let the symbols be the same as before*:

$$S(\theta^a) = \begin{cases} S(\theta), & a \in D_0, \\ S(\theta) + 1, & a \in D_1, \\ 1 + \left(\dfrac{p-1}{2} \bmod 2\right), & a \in P, \\ \left(\dfrac{q-1}{2} \bmod 2\right), & a \in Q. \end{cases}$$

Proof. By Lemma 1, $aD_0 = D_0$ if $a \in D_0$. If $a \in D_0$, $aP = P$ since $\gcd(a, q) = 1$. Hence

$$\begin{aligned} S(\theta^a) &= \sum_{i \in P} \theta^{ai} + \sum_{i \in D_1} \theta^{ai} \\ &= \sum_{i \in P} \theta^i + \sum_{j \in D_1} \theta^j \\ &= S(\theta). \end{aligned}$$

If $a \in D_1$, by Lemma 1 $aD_1 = D_0$. Note that

$$\left(\sum_{i \in D_0} + \sum_{i \in D_1} + \sum_{i \in P} + \sum_{i \in Q} \right) \theta^i + 1 = \sum_{i=0}^{N-1} \theta^i = 0.$$

By (4) and (5), together with Lemma 2 we obtain

$$\begin{aligned} S(\theta^a) &= \sum_{i \in P} \theta^{ai} + \sum_{i \in D_1} \theta^{ai} \\ &= \sum_{i \in P} \theta^i + \sum_{j \in aD_1} \theta^j \\ &= S(\theta) + 1 + \sum_{i \in Q} \theta^i + \sum_{i \in P} \theta^i \\ &= S(\theta) + 1. \end{aligned}$$

If $a \in P$, then $aP = P$ since $\gcd(p, q) = 1$. Then by Lemma 2

$$\begin{aligned} S(\theta^a) &= \sum_{i \in P} \theta^{ai} + \sum_{i \in D_1} \theta^{ai} \\ &= \sum_{i \in P} \theta^i + \sum_{i \in D_1} \theta^{ai} \\ &= 1 + \left(\frac{p-1}{2} \bmod 2 \right). \end{aligned}$$

If $a \in Q$, then $aP = \{0\}$. Then by Lemma 2

$$\begin{aligned} S(\theta^a) &= \sum_{i \in P} \theta^{ai} + \sum_{i \in D_1} \theta^{ai} \\ &= [(q-1) \bmod 2] + \sum_{i \in D_1} \theta^{ai} \\ &= \left(\frac{q-1}{2} \bmod 2 \right). \end{aligned}$$

This completes the proof of this lemma. ■

Note also that

$$S(1) = [q - 1 + (p - 1)(q - 1)/2] \bmod 2 = 0. \tag{6}$$

LEMMA 4. *$2 \in D_0$ if and only if $S(\theta) \in \{0, 1\}$.*

Proof. By (4) and definition

$$\begin{aligned} S(\theta) &= \sum_{i \in P} \theta^i + \sum_{i \in D_1} \theta^i \\ &= 1 + \sum_{i \in D_1} \theta^i. \end{aligned}$$

Since the field $GF(2^m)$ has characteristic 2, if $2 \in D_0$ then $2D_i = D_i$ for each i. By Lemma 3

$$S(\theta) = S(\theta^2) = 1 + \sum_{i \in D_1} \theta^{2i} = S(\theta).$$

Hence, $S(\theta) = 0$ or 1.

If $2 \in D_1$, then by Lemma 3 we have, similarly,

$$S(\theta)^2 = S(\theta^2) = 1 + \sum_{i \in D_1} \theta^{2i} = 1 + S(\theta).$$

Hence, $S(\theta) \notin \{0, 1\}$. Since $2 \in D_0 \cup D_1$, we have completed the proof. ■

In the sequel, we need the following generalized Chinese Remainder Theorem.

LEMMA 5. *Let m be the least common multiple of two positive integers m_1 and m_2. The system of congruences*

$$x \equiv a_1 \,(\mathrm{mod}\, m_1), \qquad x \equiv a_2 \,(\mathrm{mod}\, m_2) \tag{7}$$

has solutions if and only if

$$\gcd(m_1, m_2) | a_1 - a_2, \tag{8}$$

where $a|b$ means that a divides b. When the condition (8) *holds, the system of congruences of* (7) *has only one solution modulo m.*

For a proof of this theorem, we refer to [5].

LEMMA 6. *$2 \in D_0$ if and only if $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 1 \pmod 8$ or $p \equiv \pm 3 \pmod 8$ and $q \equiv \pm 3 \pmod 8$.*

Proof. Assume that $2 \in D_0$. By definition there is an integer s with $0 \le s \le e - 1$ such that $2 = (g^s \bmod pq)$. It follows that

$$g^s \equiv 2 \pmod p, \qquad g^s \equiv 2 \bmod q.$$

If s is even, then 2 is a quadratic residue modulo both p and q. Hence, by the Law of Quadratic Reciprocity $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 1 \pmod 8$.

If s is odd, then 2 is a quadratic nonresidue modulo both p and q. Hence, by the Law of Quadratic Reciprocity $p \equiv \pm 3 \pmod 8$ and $q \equiv \pm 3 \pmod 8$. This proves the necessity.

If $p \equiv \pm 1 \pmod 8$ and $q \equiv \pm 1 \pmod 8$. Then 2 is a quadratic residue modulo both p and q. Thus, there are even s_1 and even s_2 with $0 \le s_1 \le p - 1$ and $0 \le s_2 \le q - 1$ such that

$$g^{s_1} \equiv 2 \,(\mathrm{mod}\, p), \qquad g^{s_2} \equiv 2 \,(\mathrm{mod}\, q). \tag{9}$$

Note that $\gcd(p - 1, q - 1) = 2$ and s_1 and s_2 both are even. By the generalized Chinese Remainder Theorem described in Lemma 5, there is an integer s with $0 \le s \le e - 1$ such that

$$s \equiv s_1 \pmod{p - 1}, \qquad s \equiv s_2 \pmod{q - 1}.$$

This s is unique. Hence, $g^2 \equiv 2 \pmod{pq}$, and $2 \in D_0$.

If $p \equiv \pm 3 \pmod 8$ and $q \equiv \pm 3 \pmod 8$, we can similarly prove that $2 \in D_0$. ∎

Let θ be the same as before. Among the pq pqth roots of unity θ^i, where $0 \le i \le pq - 1$, the q elements θ^i, $i \in P \cup R$, are qth roots of unity, the p elements θ^i, $i \in Q \cup R$, are pth roots of unity. Hence,

$$x^p - 1 = \prod_{i \in Q \cup R} (x - \theta^i), \qquad x^q - 1 = \prod_{i \in P \cup R} (x - \theta^i).$$

Let

$$d(x) = \prod_{i \in D_0 \cup D_1} (x - \theta^i).$$

It follows that

$$x^{pq} - 1 = \prod_{i=0}^{pq-1} (x - \theta^i) = \frac{(x^p - 1)(x^q - 1)}{x - 1}\, d(x),$$

where $d(x) \in GF(2)[x]$.

In the sequel let L and $m(x)$ denote the linear complexity and minimal polynomial of our generalized cyclotomic sequence of order 2 with respect to the two prinmes p and q.

THEOREM 1. (I) *If* $p \equiv 1 \pmod 8$ *and* $q \equiv 3 \pmod 8$ *or* $p \equiv -3 \pmod 8$ *and* $q \equiv -1 \pmod 8$, *then*

$$L = pq - 1, \qquad m(x) = \frac{x^{pq} - 1}{x - 1}.$$

(II) *If* $p \equiv -1 \pmod 8$ *and* $q \equiv 3 \pmod 8$ *or* $p \equiv 3 \pmod 8$ *and* $q \equiv -1 \pmod 8$, *then*

$$L = (p - 1)q, \qquad m(x) = \frac{x^{pq} - 1}{x^q - 1}.$$

(III) *If* $p \equiv -1 \pmod 8$ *and* $q \equiv -3 \pmod 8$ *or* $p \equiv 3 \pmod 8$ *and* $q \equiv 1 \pmod 8$, *then*

$$L = pg - p - q + 1 \qquad m(x) = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

Proof. Note that $\gcd(p - 1, q - 1) = 2$. By Lemma 6 the six cases described in this theorem are the only ones such that $\gcd(p - 1, q - 1) = 2$ and $2 \notin D_0$.

In the two cases of (I), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ \neq 0, & a \in D_0 \cup D_1 \text{ (by Lemma 6)}, \\ 1, & a \in P \cup Q. \end{cases}$$

Hence, $\gcd(x^{pq} - 1, S(x)) = x - 1$. It follows that

$$m(x) = \frac{x^{pq} - 1}{\gcd(x^{pq} - 1, S(x))} = \frac{x^{pq} - 1}{x - 1},$$

$$L = \deg(m(x)) = pq - 1.$$

In the two cases of (II), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ \neq 0, & a \in D_0 \cup D_1 \text{ (by Lemma 6)}, \\ 0, & a \in P, \\ 1, & a \in Q. \end{cases}$$

Hence, $\gcd(x^{pq} - 1, S(x)) = x^q - 1$. It follows that

$$m(x) = \frac{x^{pq} - 1}{\gcd(x^{pq} - 1, S(x))} = \frac{x^{pq} - 1}{x^q - 1},$$
$$L = \deg(m(x)) = pq - q = (p - 1)q.$$

In the two cases of (III), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ \neq 0, & a \in D_0 \cup D_1 \text{ (by Lemma 6)}, \\ 0, & a \in P \cup Q. \end{cases}$$

Hence, $\gcd(x^{pq} - 1, S(x)) = (x^p - 1)(x^q - 1)/(x - 1)$. It follows that

$$m(x) = \frac{x^{pq} - 1}{\gcd(x^{pq} - 1, S(x))} = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)},$$
$$L = \deg(m(x)) = pq - p - q + 1. \quad \blacksquare$$

Define

$$d_a(x) = \prod_{i \in D_a} (x - \theta^i), \qquad a = 0, 1.$$

In case $2 \in D_0$, by Lemma 1 we have $2D_0 = D_0$ and

$$\begin{aligned} d_0(x)^2 &= \prod_{i \in D_0} (x^2 - \theta^{2i}) \\ &= \prod_{j \in 2D_0} (x^2 - \theta^j) \\ &= \prod_{j \in D_0} (x^2 - \theta^j) \\ &= d_0(x^2). \end{aligned}$$

Hence, $d_0(x) \in GF(2)[x]$. Similarly, we can prove that $d_1(x) \in GF(2)[x]$.

By definition

$$d(x) = d_0(x)d_1(x).$$

Thus, in case $2 \in D_0$ we get

$$x^{pq} - 1 = \frac{(x^p - 1)(x^q - 1)d_0(x)d_1(x)}{x - 1}. \tag{10}$$

Note that $d_0(x)$ and $d_1(x)$ depend on the choice of θ. However, by Lemmas 3 and 4, exactly one of $S(\theta)$ and $S(\theta^a)$ is zero, where a is an element of D_1. Thus, we can choose our θ such that $S(\theta) = 0$. With this choice we can fix the polynomials $d_0(x)$ and $d_1(x)$.

THEOREM 2 (IV). *If* $p \equiv 1 \pmod 8$ *and* $q \equiv -1 \pmod 8$ *or* $p \equiv -3 \pmod 8$ *and* $q \equiv 3 \pmod 8$, *then*

$$L = \frac{pq + p + q - 3}{2}, \qquad m(x) = \frac{x^{pq} - 1}{(x - 1)d_0(x)}.$$

(V) *If* $p \equiv -1 \pmod 8$ *and* $q \equiv 1 \pmod 8$ *or* $p \equiv 3 \pmod 8$ *and* $q \equiv -3 \pmod 8$, *then*

$$L = \frac{(p - 1)(q - 1)}{2}, \qquad m(x) = d_1(x).$$

(VI) *If* $p \equiv -1 \pmod 8$ *and* $q \equiv 1 \pmod 8$ *or* $p \equiv 3 \pmod 8$ *and* $q \equiv 3 \pmod 8$, *then*

$$L = \frac{(p - 1)(q + 1)}{2}, \qquad m(x) = \frac{(x^p - 1)d_1(x)}{x - 1}.$$

Proof. By Lemma 6 there are eight cases such that $2 \in D_0$, but two of them do not satisfy $\gcd(p - 1, q - 1) = 2$. It is easy to check that the six cases described in this theorem are the only ones such that $2 \in D_0$ and $\gcd(p - 1, q - 1) = 2$.

In the two cases of (IV), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ 0, & a \in D_0 \text{ (by the choice of } \theta), \\ 1, & a \in D_1 \text{ (by the choice of } \theta), \\ 1, & a \in P \cup Q \text{ (by Lemma 3)}. \end{cases}$$

Hence,

$$\gcd(x^{pq}-1, S(x)) = (x-1)d_0(x),$$
$$m(x) = \frac{x^{pq}-1}{\gcd(x^{pq}-1, S(x))} = \frac{x^{pq}-1}{(x-1)d_0(x)},$$
$$L = \deg(m(x)) = pq - 1 - (p-1)(q-1)/2$$
$$= (pq + p + q - 3)/2.$$

In the two cases of (V), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ 0, & a \in D_0 \text{ (by the choice of } \theta), \\ 1, & a \in D_1 \text{ (by the choice of } \theta), \\ 1, & a \in P \cup Q \text{ (by Lemma 3)}. \end{cases}$$

Hence,

$$\gcd(x^{pq}-1, S(x)) = \frac{(x^p-1)(x^q-1)d_0(x)}{x-1},$$
$$m(x) = \frac{x^{pq}-1}{\gcd(x^{pq}-1, S(x))} = d_1(x),$$
$$L = \deg(m(x)) = \frac{(p-1)(q-1)}{2}.$$

In the two cases of (VI), by Lemma 3

$$S(\theta^a) = \begin{cases} 0, & a = 0 \text{ (by (6))}, \\ 0, & a \in D_0 \text{ (by the choice of } \theta), \\ 1, & a \in D_1 \text{ (by the choice of } \theta), \\ 0, & a \in P \text{ (by Lemma 3)}, \\ 1, & a \in Q \text{ (by Lemma 3)}. \end{cases}$$

Hence,

$$\gcd(x^{pq}-1, S(x)) = (x^q-1)d_0(x),$$
$$m(x) = \frac{x^{pq}-1}{\gcd(x^{pq}-1, S(x))} = \frac{(x^p-1)d_1(x)}{x-1},$$
$$L = \deg(m(x)) = pq - \frac{(p-1)(q-1)}{2} - q$$
$$= \frac{(p-1)(q-1)}{2}. \quad \blacksquare$$

It is known that the average linear complexity of binary sequences of period n is about $n - 1$ and that of binary finite sequences of length n is about $n/2$ [13]. The two theorems show that the linear complexity is rather good.

The sequence defined here is the complement of the original one defined in [4], i.e., the exclusive-or of this sequence with the original one defined in [4] is an all–one constant sequence. Thus, the linear complexity of the original generalized cyclotomic sequence of order 2 is equal to that of this one plus one.

3. HARDWARE IMPLEMENTATION AND APPLICATION

This paper only aims at the computation of the linear complexity of the generalized cyclotomic binary sequences of order 2. In this section we only outline a hardware implementation of the two-prime cyclotomic generator of order 2 that outputs the generalized cyclotomic sequence of order 2 concerned in this paper.

By the Chinese Remainder Theorem the sequence concerned in this paper is an output sequence of the generator described in Fig. 1, where CC1 and CC2 denote two cyclic counters that count the numbers $\{0, 1, 2, \ldots, p - 1\}$ and $\{0, 1, 2, \ldots, q - 1\}$ cyclically, respectively, and within CC1 and CC2 there are registers R1 and R2 that store the current counted number. The initial contents k_1 and k_2 of the two registers form the key of this generator, i.e., $k = (k_1, k_2)$, where $0 \le k_1 \le p - 1$ and $0 \le k_2 \le q - 1$. Cyclic counters are very efficient and frequently are seen in modern electronic devices. In Fig. 1 MEC1 and MEC2 are two special chips for modular exponentiation with respect to p and q, respectively. They are similar to RSA chips [14, p. 469] and can also be made relatively efficient as the two primes here are much smaller than those for an RSA public-key cryptosystem. Here we use primes having about 46 bits, while in RSA at least 512-bit primes are needed. MEC1 and MEC2 compute $x^{(p-1)/2} \bmod p$ and $y^{(q-1)/2} \bmod q$, respectively. The u_0 and v_0 denote the least significant bits of the output numbers of MEC1 and MEC2, respectively, and u_1 and v_1 the next bits of u_0 and v_0, respectively. Finally, $\otimes$ and $\oplus$ denote the binary multiplier and adder that realize the multiplication and addition of $\mathrm{GF}(2) = \{0, 1\}$.

The correctness of this implementation is proved as follows. For each $0 \le j \le pq - 1$ let

$$u = j^{(p-1)/2} \bmod p \in \{0, 1, p - 1\},$$
$$v = j^{(q-1)/2} \bmod q \in \{0, 1, q - 1\}.$$

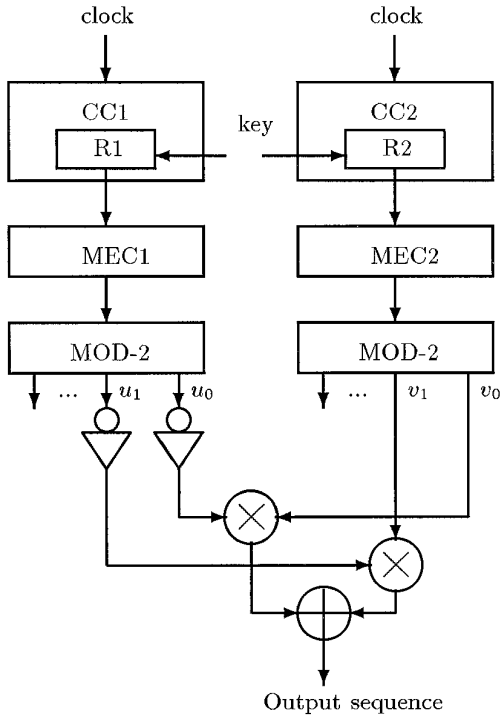

FIG. 1. A hardware implementation of the two two-prime cyclotomic generator.

By the definitions of u_0, u_1, v_0, v_1, and s_j, we have the following correspondence depicted by Table 1. It is easily seen that

$$s_j = (u_1 \oplus 1) \otimes v_1 \oplus (u_0 \oplus 1) \otimes v_0.$$

TABLE 1
The Relations

(u, v)	(u_1, u_0, v_1, v_0)	s_j
$(1, 1)$	$(0, 1, 0, 1)$	0
$(1, q-1)$	$(0, 1, 1, 0)$	1
$(p-1, 1)$	$(1, 0, 0, 1)$	1
$(p-1, q-1)$	$(1, 0, 1, 0)$	0
$(0, 1)$	$(0, 0, 0, 1)$	1
$(0, q-1)$	$(0, 0, 1, 0)$	1
$(1, 0)$	$(0, 1, 0, 0)$	0
$(p-1, 0)$	$(1, 0, 0, 0)$	0
$(0, 0)$	$(0, 0, 0, 0)$	0

Then the correctness of this implementation follows from the Chinese Remainder Theorem.

The additive synchronous stream cipher based on this generator is as usual. For this purpose we suggest to use two 48-bit primes, then the keysize is 96 bits that should be large enough as far as brute-force attack is concerned. Twin primes might be better than others. With current chips for modular exponentiation with respect to such primes [14, p. 469], this specific cipher should be able to encrypt and decrypt at least 30 Kbytes per second. Note that one page of English text (A4 size, ASCII) is about 3 Kbytes. Thus, such a cipher could encrypt 10 pages of English text per second. This performance may be slow for multimedia applications, but certainly reasonable in military and diplomatic communications, where the data in communication is usually not very large, say less than 600 pages of English text in each communication. Note that ciphering a 600-page document takes only one minute. It can also be used to encrypt and decrypt classified large data base where performance is not so important, but secrecy is the primary concern.

Traditional stream ciphers are usually based on shift registers, but correlation attacks might be applicable to them [3, 15, 16]. Recently, there are some software-oriented fast-stream ciphers such as SEAL [12], WAKE [18], and the alleged RC4 [14, pp. 397–398]. They are really fast in software, but no statistical property of them is known. Note that we do not even known the least period of the keystream of the alleged RC4. With a number of statistical properties described in this paper and [4], we expect that the above specific cipher provides high security. This paper is not about this cipher, but about the linear complexity of the output sequences of the two-prime cyclotomic generator. However, it would be good to outline a hardware implementation and point out some applications. Finally, we mention that the two-prime cyclotomic generator has the same level of performance as the Blum–Blum–Shub generator [2].

ACKNOWLEDGMENT

The author thanks the two anonymous referees for their detailed and very helpful comments and suggestions that much improved this paper.

REFERENCES

1. L. D. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, New York/Berlin, 1971.
2. L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudo-random number generator, *SIAM J. Comput.* **15** (1986), 364–383.

3. C. Ding, G. Xiao, and W. Shan, "The Stability Theory of Stream Ciphers," Lect. Notes in Comput. Sci., Vol. 561, Springer-Verlag, New York/Berlin, 1991.
4. C. Ding, Binary cyclotomic generators, *in* "Fast Software Encryption" (B. Preneel, Ed.), Lect. Notes in Comput. Sci. Vol. 1008, pp. 29–60, Springer-Verlag, New York/Berlin, 1995.
5. C. Ding, D. Pei, and A. Salomaa, "Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography," Section 2.4, World Scientific, Singapore, 1996.
6. C. F. Gauss, "Disquisitiones Arithmeticae," English transl., Yale Univ. Press, New Haven, CT, 1966; reprint, Springer-Verlag, Berlin/Heidelberg/New York, 1986.
7. R. Lidl and H. Niederreiter, "Finite Fields," Addison–Wesley, Reading, MA, 1983.
8. H. Niederreiter, Sequences with almost perfect linear complexity profile, *in* "Advances in Cryptology: Proc. Eurocrypt'87," Lect. Notes in Comput. Sci., Vol. 304, pp. 37–51, Springer-Verlag, New York/Berlin, 1988.
9. H. Niederreiter, Keystream sequences with a good linear complexity profile for every starting point, *in* "Advances in Cryptology: Proc. Eurocrypt'89," Lect. Notes in Comput. Sci., Vol. 434, pp. 523–532, Springer-Verlag, New York/Berlin, 1990.
10. H. Niederreiter, A combinatorial approach to probabilistic results on the linear complexity profile of random sequences, *J. Cryptology* **2** (1990), 105–112.
11. H. Niederreiter, The linear complexity profile and the jump complexity of keystream sequences, *in* "Advances in Cryptology: Proc. Eurocrypt'90," Lect. Notes in Comput. Sci., Vol. 473, pp. 174–188, Springer-Verlag, New York/Berlin, 1991.
12. P. Rogaway and D. Coppersmith, A software-oriented encryption algorithm, *in* "Fast Software Encryption," Lect. Notes in Comput. Sci., Vol. 809, pp. 56–63, Springer-Verlag, New York/Berlin, 1994.
13. R. A. Rueppel, Linear complexity and random sequences, *in* "Advances in Cryptology: Eurocrypt'85," Lect. Notes in Comput. Sci., Vol. 219, pp. 167–188, Springer-Verlag, New York/Berlin, 1986.
14. B. Schneier, "Applied Cryptography," 2nd ed., Wiley, New York, 1996.
15. T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, *IEEE Trans. Comput.* **C-34** (1985), 81–85.
16. T. Siegenthaler, Cryptanalyst's representation of nonlinearly filtered ml-sequences, *in* "Advances in Cryptology: Proc. of Eurocrypt'85" (F. Pichler, ed.), Lect. Notes in Comput. Sci., Vol. 219, pp. 103–110, Springer-Verlag, New York/Berlin, 1986.
17. T. Storer, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.
18. D. J. Wheeler, A bulk data encryption algorithm, *in* "Fast Software Encryption," Lect. Notes in Comput. Sci., Vol. 809, pp. 127–134, Springer-Verlag, New York/Berlin, 1994.
19. A. L. Whiteman, A family of difference sets, *Illinois J. Math.* **6** (1962), 107–121.